CYBERFEED

A POWERFUL SOLUTION PROVIDING ACTIONABLE THREAT INTELLIGENCE ON THE FIGHT AGAINST BOTNETS

anubisnetworks™
a BITSIGHT company

↘ CUSTOMER
CASE STUDY

Customer is:

A Computer Emergency Response Team (CERT) based in the South of Europe that identifies and remediates security incidents, such as botnet infections and malware, affecting enterprise organizations.

OBJECTIVE

This CERT is tasked to defend its nation's critical infrastructure and, at the same time, provide insight on the Country Threat Landscape. They wanted accurate intelligence on the main attack vector - Malware Infections - without false positives, and with enough breadth to cover the entire country. This intelligence (feed) would be the baseline KPI for doing their malware detection work.

Being specialized in the detection of cyber-threats, this entity objective was also to ensure that the threat-intelligence was actionable (allowing remediation) and on-time, for a quicker risk mitigation. In the end, the Country goal is to improve the security level on a nationwide scale.

Moreover, this CERT wanted to implement a "National Anti-Botnet Support Centre", by accelerating how botnets were discovered, and sending accurate reports to organizations, thus gaining a nationwide insight on their constituents, but also on the country and industries.

CUSTOMER SOLUTION

This National CERT has selected Cyberfeed, AnubisNetworks actionable threat-intelligence solution which provides real-time events, and a unique view in the early detection of cyber-threats.

They have used Cyberfeed real-time events, accessed via API, and normalized to be combined with other intelligence (open source feeds and log-related indicators) in their Event Manager system.

Cyberfeed data enabled this CERT to gain new insights and augmented its ability to track and monitor botnets.

Thus, this entity was able to decrease significantly the time needed to mitigate cyber-risk, by detecting devices and machines related to information stealing Trojans.

This CERT also raised its visibility over certain types of botnets, which before were untraceable, hence protecting more organizations and enlarging its activity scope.

This expanded visibility led to adding quality and functionalities to the "National Anti-Botnet Support Center", by allowing this project to detect botnets communications in real-time.

Cyberfeed helped to expand the depth and quality of data to prevent security events. In addition, the actionability of the data - due to the context provided - helped decreasing the response times among organizations in this CERT's country to very adequate levels.

> **"We were looking for a reference company in the Botnet detection, and Anubisnetworks showed us a great threat intelligence solution, by being quick and, accurate in delivering a cyber security service with a high quality"**
>
> **CERTs Director**

BUSINESS BENEFITS

This CERT was looking for a solution which allowed it better do their work, by obtaining actionable and contextualized insights into security threats. This CERT has understood the need to use a proprietary, high quality source, with the corresponind advantages: real-time streaming of events, improved quality, broader scope, and, of course, support, and robustness they could not find with open sources.

By using Cyberfeed, this CERT could truly experience business benefits, obtaining very low false-positives rates and enriched event information which augmented their perceived expertise among their constituens.

Additionally, it was possible to put data into real action through instant sharing of infection details and remediation information to critical infrastructure organizations, preventing serious attacks on their country.

Also due to Cyberfeed, the "National Anti-Botnet Support Center" is very successful, as it empowers organizations to act quickly, and delivering a better understanding of the threat landscape and infection activity.

According to this CERT's Director,

> "By creating a comprehensive picture of cybercrime, it could then be possible to generate timely and accurate ground level assessments. Cyberfeed definitely empowers organizations to fight cyber criminals, by providing real-time data on cyber-attacks, allowing organizations to mitigate risks as they arise".

WHAT HAS CONVINCED THE CUSTOMER

More than 25 000 events per second collected and streamed to security feeds as they happen.

Turning data into actionable intelligence is the cornerstone of Cyberfeed. Events collected from disparate sources, including botnets only tracked by AnubisNetworks, are transformed and enriched into meaningful knowledge to help stop cyber threats and attacks.

It dynamically provides full context of what is happening and not a snapshot of the past, enabling cybersecurity analysts to obtain increased visibility into a situation and allowing informed decision-making.

Cyberfeed API flexibility allows customizing and processing data feeds in real-time, including measuring, filtering and de-duplicating events on the fly. Cybersecurity analysts can slice and dice data to better fit their requirements and build the necessary knowledge to stop threats.

Provides real-time data on cyber-attacks, allowing organizations to mitigate risks as they arise.

Since the information is processed in real-time, users do not need to invest in data storage, making this a lean and very light service.

FOR MORE INFORMATION ABOUT CYBERFEED, PLEASE VISIT OUR WEBSITE @ **HTTP://WWW.ANUBISNETWORKS.COM**

twitter.com/anubisnetworks

linkedin.com/company/anubisnetworks

youtube.com/user/anubisnetworks

↘ REACH US

PORTO
Address
UPTEC, Rua Alfredo Allen 455/461,
Sala EC.3.12, 4200-135 Porto, Portugal
Phone: +351 220 993 873

LISBON
Address
Av. D. João II, Lote 1.07.2.1, 4th Floor, Parque
das Nações, 1998-014, Lisbon, Portugal
Phone: +351 217 252 110

BOSTON
Address
125 CambridgePark Drive
Suite 204, Cambridge, MA 02140l
Phone: +1 617 245 0469

AnubisNetworks is a CyberSecurity Company specialized in real-time threat Intelligence, and with an established reputation for delivering innovative and effective solutions. AnubisNetworks solutions are fitted for service providers, risk and security organizations, telcos, major banks, National CERTs, Defense and Homeland Security, looking for real-time Insight on Infections and Vulnerabilities.

anubisnetworks™
a BITSIGHT company